Our Lady of Perpetual Succour Catholic Primary School, a Voluntary Academy

e-Safeguarding Policy

This policy was approved by…

Staff: September 2017

Governors: October 2017

Review date: Autumn 2019

OUR LADY OF PERPETUAL SUCCOUR CATHOLIC PRIMARY ACADEMY

SCHOOL INTERNET SAFEGUARDING POLICY (e-Safeguarding)

1. Introduction

Our Lady of Perpetual Succour Catholic Primary Academy fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of internet and electronic communication technology such as mobile phones and wireless connectivity. The internet and other technologies have an important role in the learning and teaching processes however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school e-Safeguarding Policy will operate in conjunction with others including: policies for Safeguarding, Behaviour, Anti-Bullying, Equality and Acceptable Use Agreements with staff, pupils and parents.

The school acknowledges e-safety and e-security as important issues for our school community and has made a considered attempt to embed e-safeguarding into our teaching and learning using technology and have considered the wider implications of e-safeguarding beyond classroom practice such as security and data.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safeguarding Policy;
- Secure, filtered broadband from the company Capital Bytes that uses 'Netsweeper'
- The use of e-safety control software monitoring system which monitors and captures inappropriate words or web sites used, including those associated with the PREVENT duty

Writing and Reviewing the e-Safeguarding Policy

The e-Safeguarding Policy is part of the School Development Plan and relates to other policies including those for ICT, anti-bullying and for child protection

Mr John Williams is the school's e-Safety Leader.

- Our e-Safeguarding Policy has been written by the school, building on the Yorkshire and Humberside e-Safeguarding Policy. It has been agreed by staff and approved by governors.
- It was reviewed and approved by the Governors in February 2016
- The next review date is (at least annually): Spring Term 2017

2. Our Aims

- To set out the key principles expected of all members of the school community at Our Lady of Perpetual Succour Catholic Primary Academy with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Our Lady of Perpetual Succour Catholic Primary Academy.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

3. Scope of Policy

- This policy applies to the whole school community including Our Lady of Perpetual Succour Catholic Primary Academy's Senior Leadership Team, school board of Governors, all staff employed directly or indirectly by the school, volunteers and all pupils.
- Our Lady of Perpetual Succour Catholic Primary Academy's Senior Leadership Team and school board of Governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other e-Safeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy and the anti-bullying policy and will, where known, inform parents and carers of

incidents of inappropriate e-Safeguarding behaviour that takes place out of school.

4. Review and Ownership

- The school has appointed an e-Safeguarding leader (Mr John Williams) who will be responsible for document ownership, review and updates.
- The e-Safeguarding policy has been written by the school e-Safeguarding leader, alongside the Senior Leadership Team, and is current and appropriate for its intended audience and purpose.
- The e-Safeguarding policy is reflected in many other school policies such as the ICT policy, Child Protection policy, Anti-bullying policy and the School Improvement Plan.
- The school e-Safeguarding policy has been agreed by the Senior Leadership Team and approved by governors.
- The e-Safeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

5. Communication Policy

- Our Senior Leadership Team and class teachers will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school e-Safeguarding policy and the use of any new technology within school.
- The e-Safeguarding policy will be provided to and discussed with all members of staff and reviewed annually.
- We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used
- The e-Safeguarding policy will be introduced to the pupils at the start of each school year

6. Roles and Responsibilities

6.1. Responsibilities of the school community

We believe that e-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

- The Senior Leadership Team
- The e-Safeguarding Leader
- Teachers and upport staff
- ICT technician and technical staff
- Pupils
- Parents and carers
- Governing body
- Child Protection Designated Persons
- External groups

6.2. Responsibilities of the Senior Leadership Team

- The Headteacher is ultimately responsible for e-Safeguarding provision including e-Safeguarding for all members of the school community as is our designated e-Safeguarding Leader.
- The Headteacher and Senior Leadership Team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their e-Safeguarding roles and to train other colleagues when necessary.

6.3. Responsibilities of the e-Safeguarding Leader

- To promote an awareness and commitment to e-Safeguarding throughout the school
- To be the first point of contact in school on all e-Safeguarding matters
- To take day-to-day responsibility for e-Safeguarding within school and to have a leading role in establishing and reviewing the school e-Safeguarding policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the designated e-Safeguarding Governor
- To create and maintain e-Safeguarding policies and procedures
- To ensure that all members of staff receive an appropriate level of training in e-Safeguarding issues
- To ensure that e-Safeguarding education is embedded across the curriculum
- To ensure that e-Safeguarding is promoted to parents and carers
- To liaise with the Local Authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safeguarding incident
- To ensure that an e-Safeguarding incident log is kept up to date
- To ensure that the school Acceptable Use policies are current and pertinent.

6.4 Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the e-Safeguarding Leader
- To develop and maintain an awareness of current e-Safeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed e-Safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

6.5 Responsibilities of ICT technician/technical staff

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any e-Safeguarding related issues that come to your attention to the e-Safeguarding Leader.
- To develop and maintain an awareness of current e-Safeguarding issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues

- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted

6.6 Responsibilities of pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To know and understand school policies regarding cyber bullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to – using the SMART rules
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school

6.7 Responsibilities of parents and carers

- To help and support the school in promoting e-Safeguarding
- To read, understand and promote the school pupil Acceptable Use Policy with their children
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the school's permissions form which clearly sets out the use of photographic and video images outside of school

- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school
- Parents and carers are required to give written instruction if they do NOT wish for any images of their child to be used.

6.8 Responsibilities of the Governing body

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school
- To ensure appropriate funding and resources are available for the school to implement its e-Safeguarding strategy

6.9 Responsibilities of the Child Protection Designated Person

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyber bullying and the use of social media for this purpose

6.10 Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to e-safeguarding and the safe use of technologies
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds

- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school

7. Managing Digital Content

7.1 Using images, video and sound

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done via the permissions form included in the welcome pack for new starters.
    1. On the school website
    2. In the school prospectus and other printed promotional material, e.g. newsletters
    3. In display material that may be used around the school
    4. In display material that may be used off site
    5. Recorded or transmitted on a video or via webcam in an educational conference
- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

7.2 Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network or school owned cloud storage and never transferred to personally-owned equipment.
- The school may store images of pupils that have left the school following their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- All staff have the responsibility of deleting the images when they are no longer required.

8. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a series of specific e-Safeguarding-related lessons in specific year groups as part of the ICT curriculum / PSHE curriculum.
- We will celebrate and promote e-Safeguarding through whole-school activities, including promoting Safer Internet Day.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or

carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse icon.

8.1. Staff Training

- Our staff receive regular information and training on e-Safeguarding issues in the form of annual updates, staff meetings etc.
- As part of the induction process all new staff receive information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-Safeguarding activities and awareness within their curriculum areas

9. Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Pupils will access the internet using year group logins, which the teacher supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

10. Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly-chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen or a school's or local authority's network being infected or attacked. The school has a responsibility to ensure that all elements of the school infrastructure and network equipment are as safe and secure as possible. All staff and pupil access to school-owned equipment and information assets should be controlled through the use of appropriate username and password complexity policies.

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Pupils will have a generic year group logon to all school ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords. Staff are reminded that they:
    1. Do not write down system passwords.
    2. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    3. Always use your own personal passwords to access computer based services, never share these with other users.
    4. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    5. Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.

- The school maintains a log of all accesses by users and of their activities while using the system.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

11. Emerging Technologies

New and emerging technologies are being developed constantly in today's fast-moving digital world. These technologies can be anything from handheld devices to new faster communication mechanisms. Schools should try to always be aware of new and appealing technologies as these can, in many cases, offer the potential to develop new teaching and learning tools.

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safeguarding point of view. We will regularly amend the e-Safeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-Safeguarding risk.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- Emerging technologies can incorporate software and/or hardware products.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the e-Safeguarding policy is adequate and that the implementation of the e-Safeguarding policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

12. Filtering Internet Access

As all schools will be aware, the internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose internet filtering

solution is deployed. As with any aspect of education, decisions and guidance from OFSTED very much influence what schools need and want. The OFSTED report, 'Safe use of new technologies' (February 2010) had, as one of its key findings, 'Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.'

- The school uses a filtered internet service. The filtering system is provided by Capital Bytes.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safeguarding Leader. All incidents should be documented.
- The school will regularly review the filtering product for its effectiveness.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

13. Internet Access Authorisations

Schools should allow internet access to staff and pupils on the grounds that it is required for either work-related purposes or for educational need. The school should keep a record of who has access to the internet and what internet filtering policy will be applied to the individual user. By documenting access requests and authorisations a school has a full audit trail of when and to whom access has been granted.

- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.

- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.
- Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.
- Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

14. Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place.

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils will be allocated an individual email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents. (unless granted permission from the Headteacher)
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

14.1 Email usage

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- All confidential documents send between staff via email will be password protected.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.
- Chain messages will not generally be permitted (please check with the Headteacher) or forwarded on to other school-owned email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations or parents, are advised to carbon copy (cc) or include the Headteacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.

15. Using Blogs, Wikis, Podcasts, Social Networking and Other

Ways for Pupils to Publish Content Online

We use blogs and other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within secure areas on the school website.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the school website and postings should be approved by the Headteacher before publishing.

- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

16. Mobile Phone Usage in School

In today's digital world, communications and content are available almost anywhere at any time. Gone are the days when mobile phones could only be used for making phone calls. They are now multi-functional, smart devices which can be used for browsing the internet, email, texting, mobile applications, social networking, photography and video. Modern-day smart phones are effectively mobile computers, which are far more powerful and feature-rich devices than the original home computers.

16.1 General issues

- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time.
- Mobile phones and personally owned mobile devices brought in to school by staff are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Pupils are not permitted to bring mobile phones to school

16.2 Pupils' use of personal devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones will be released to parents or carers in accordance with the school policy.

16.3 Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- Staff are not permitted to use their mobile phones in school when there are children present.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose (unless otherwise agreed by the headteacher).
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then they may use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

17. Data Protection and Information Security

Our Lady's Academy has a current registration for data protection. As a commitment to this registration, we are complying with the Data Protection Act 1998, with guidance from their local authority. The Academy holds lots of information and data on pupils, families and on staff. The amount of information we hold is increasing all the time and, while this data can be very useful in improving the service we provide, we also have a duty of care for how we handle and control access to the sensitive and personal information and data which we hold.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to have respect for the privacy of their personal details. The legislation itself is complex and, in places, hard to understand. However, it is underpinned by a set of nine straightforward, common-sense principles. If we make sure we handle personal data in accordance with the spirit of those principles, then we will go a long way towards ensuring that you comply with the letter of the law.

- Data should be processed fairly and lawfully
- Data should be obtained only for one or more specified and lawful purposes
- Personal data held shall be adequate, relevant and not excessive
- Data should be accurate and up to date
- Data should be held no longer than for the purpose it was originally collected

- Data should be processed in accordance with individual's rights
- Data should be secured accordingly
- Appropriate technical and organisational measures should be taken to secure all data held
- Data should be transferred only to other countries with suitable or equivalent security measures.

Our Lady's Academy implements a layered approach to the protection of the information and data assets for which we are responsible.

17.1 Senior Information Risk Owner (SIRO) - Headteacher

The Senior Information Risk Owner is a senior member of staff (normally the headteacher) who is familiar with information risks and the organisation's response.

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management
- 17.2 Information Asset Owner (IAO) – Academy and Finance Officer

The role of the IAO is to understand:

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed off

Although Our Lady's Academy has appointed these key roles, the handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.

- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- The fax machine is situated within a controlled area of the school.
- All communications involving personal or sensitive information (email, fax or post) are appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

18. Management of Assets

At Our Lady's Academy we have software and hardware assets for both educational and administrative purposes. All equipment and software comes at a cost to the school and is therefore controlled and documented appropriately. The school employs Charterfields Insurance.

By maintaining valid inventories, Our Lady's Academy is in a position to extract full value from our purchases as educational activities can be based and planned around the assets we hold. It should also not be overlooked that recording information on all equipment can also assist in hardware replacement programmes and software upgrades, as spending can be planned against asset age and specification.

The academy is aware that any old hardware such as laptops, PCs, servers and removable media needs to be formatted prior to disposal (or through a third party) to ensure no sensitive or personal data remains on old hardware.

- Details of all school owned hardware will be recorded in a hardware inventory.
- Details of all school owned software/licences will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.